

CLAIMS

WE CLAIM:

1. A method for the containment of network communication, comprising the steps of:

intercepting a message, the message sent from a client to a server over a
5 communication-conduit; and

determining whether one or more communication-conduit usage-conditions are
met.

2. The method of Claim 1, further comprising the step of forwarding the message to the
10 server over the communication-conduit when the one or more usage-conditions are met.

3. The method of Claim 2, wherein the determining step comprises identifying a first
network address of the server, a second network address of the client and a port number
of the communication-conduit.

15 4. The method of Claim 3, further comprising the step of sending a plurality of DHCP
reply messages for binding a first address of a first host to a second address of a second
host, the plurality of DHCP reply messages sent to a third host, the server residing on the
first host, and the client residing on the third host.

20 5. The method of Claim 2, wherein the determining step comprises (a) obtaining a
confirmation from a human, (b) determining whether the communication-conduit was

used by the client prior to the client's sending the message, or (c) determining whether the client sent the message within an authorized time-window.

6. The method of Claim 2, wherein the determining step comprises obtaining a
5 confirmation from a human, wherein the human (a) is associated with the client, or (b) has administrative privilege.

7. The method of Claim 2, wherein the determining step comprises (a) determining
whether the client used the communication-conduit at any time prior to the client's
10 sending the message, (b) determining whether the client used the communication-conduit within a specific time-window prior to the client's sending the message, or (c) determining whether the client used the communication-conduit within a pre-determined context prior to the client's sending the message, wherein the pre-determined context comprises a TCP connection or a session.

15

8. The method of Claim 2, wherein the determining step comprises determining whether a configuration of the client comprises one or more pre-determined data.

9. The method of Claim 2, wherein the determining step comprises determining whether
20 a repository comprises one or more authorization data pertinent to the message.

10. The method of Claim 2, wherein the determining step comprises authorizing temporary usage of the communication-conduit, wherein the temporary usage expires

unless administrative approval is obtained (a) within a pre-determined time-window, (b) before the client sends a pre-determined number of messages, or (c) before the client uses a pre-determined number of distinct contexts, wherein a context comprises a TCP connection or a session.

5

11. The method of Claim 2, wherein the determining step comprises determining whether the message is sent within a pre-determined time-window.

12. The method of Claim 11, wherein the pre-determined time-window comprises one or
10 more weekday peak usage hours.

13. The method of Claim 1, further comprising the step of discarding the message when the one or more usage-conditions are not met.

14. The method of Claim 13, wherein the determining step comprises identifying a first
15 network address of the client, a second network address of the server and a port number of the communication-conduit.

15. The method of Claim 1, further comprising the step of logging a result of the
20 determining step.

16. The method of Claim 1, further comprising the step of notifying a system-administrator of a result of the determining step.

17. A method for the containment of network communication, comprising the steps of:

intercepting a first service-request, the service-request sent from a client to a server over a network; and

5 determining whether one or more service-conditions are met.

18. The method of Claim 17, further comprising the step of forwarding the first service-request to the server over the network when the one or more service-conditions are met.

10 19. The method of Claim 18, wherein the determining step comprises identifying a first network address of the server and a second network address of the client.

20. The method of Claim 19, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the
15 first host, and the client residing on the third host.

21. The method of Claim 18, wherein the determining step comprises (a) obtaining a confirmation from a human, or (b) determining whether the client sent the first service-
20 request within an authorized time-window.

22. The method of Claim 18, wherein the determining step comprises identifying a request-type indicated by the first service-request.

23. The method of Claim 18, wherein the determining step comprises determining whether a second service-request of the same request-type as the first service-request (a) was forwarded to the server at any time prior to the client's sending the first service-request, (b) was forwarded to the server within a pre-determined time-window prior to the client's sending the first service-request, or (c) was forwarded to the server within a specific context, wherein a context comprises a TCP connection or a session.

24. The method of Claim 18, wherein the determining step comprises determining whether a second service-request of one or more pre-determined request-types (a) was forwarded to the server at any time prior to the client's sending the first service-request, (b) was forwarded to the server within a pre-determined time-window prior to the client's sending the first service-request, or (c) was forwarded to the server within a specific context, wherein a context comprises a TCP connection or a session.

15

25. The method of Claim 17, further comprising the step of discarding the first service-request when the one or more usage-conditions are not met.

26. The method of Claim 25, wherein the determining step comprises identifying a first network address of the client and a second network address of the server.

27. The method of Claim 17, further comprising the step of logging a result of the determining step.

28. The method of Claim 17, further comprising the step of notifying a system-administrator of a result of the determining step.

5 29. A system for the containment of network communication, comprising:

a communication-proxy for intercepting a message from a client to a server over a communication-conduit;

wherein the communication-proxy determines whether one or more communication-conduit usage-conditions are met, and wherein the communication-proxy

10 (a) forwards the message to the server over the communication-conduit when the one or more usage-conditions are met, or (b) discards the message when the one or more usage-conditions are not met.

30. The method of Claim 29, wherein the communication-proxy (a) obtains a
15 confirmation from a human, (b) determines whether the communication-conduit was used by the client prior to the client's sending the message, or (c) determines whether the client sent the message within an authorized time-window.

31. The system of Claim 29, wherein the communication-proxy identifies a first network
20 address of the server, a second network address of the client and a port number of the communication-conduit.

32. The method of Claim 31, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

5

33. The system of Claim 31, wherein the communication-proxy resides in a network element such as a switch or a router, the network element in a communication path between the client and the server.

10 34. The system of Claim 31, wherein the communication-proxy and the client reside on the same host.

35. The system of Claim 31, wherein the communication-proxy and the server reside on the same host.

15

36. A system for the containment of network communication, comprising:

a service-proxy for intercepting a service-request from a client to a server over a network;

wherein the service-proxy determines whether one or more service-conditions are met, and wherein the service-proxy (a) forwards the service-request to the server over the network when the one or more service-conditions are met, or (b) discards the service-request when the one or more service-conditions are not met.

20

37. The method of Claim 36, wherein the service-proxy (a) obtains a confirmation from a human, or (b) determines whether the client sent the service-request within an authorized time-window.

5 38. The system of Claim 36, wherein the service-proxy identifies a first network address of the server and a second network address of the client.

39. The method of Claim 38, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second
10 host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

40. The system of Claim 38, wherein the service-proxy resides in a network element such as a switch or a router, the network element in a communication path between the client
15 and the server.

41. The system of Claim 38, wherein the service-proxy and the client reside on the same host.

20 42. The system of Claim 38, wherein the service-proxy and the server reside on the same host.

43. The method of Claim 36, wherein the service-proxy determines a request-type indicated by the service-request.